AU/ACSC/97-0604C/97-03

AIR FORCE INFORMATION WARFARE DOCTRINE:

VALUABLE OR VALUELESS?

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Major Paul R Henning

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense.

Contents

Page

Illustrations

Page

Preface

In March 1992, the USAF published Air Force Manual 1-1, its current version of basic doctrine. The manual did not mention the term *information warfare.* In the five years since that time, information warfare has received a great deal of attention in the Department of Defense (DOD). Numerous magazine articles, books, and papers have been written within the DOD, the Joint Staff, the various Services, and corporate industry. The general consensus is that information will play a critical and ever-increasing role in how we, as a nation, perform military operations throughout the entire spectrum from peace to general war. However, there is still much "fog" associated with the topic of information warfare.

The USAF has deeply committed itself to information warfare. In 1993, it opened the Air Force Information Warfare Center, at Kelly AFB Texas, and, in 1995, formed an Information Warfare Squadron, at Shaw AFB South Carolina. Additionally, the Air Force plans to create an information warfare battle laboratory with the mission to experiment, test, exercise, and evaluate new operational concepts and systems for air and space power. To tie all of these efforts together, the Air Force is in the process of producing its first official version of information warfare doctrine. The purpose of this research paper is to answer some fundamental questions about Air Force information warfare doctrine and to examine its usefulness to Air Force members.

AU/ACSC/97-0604C/97-03

Abstract

Is Air Force information warfare doctrine valuable or valueless? This research paper answers three fundamental questions about Air Force information warfare doctrine. First, why do we need Air Force information warfare doctrine? Second, what is the status of Air Force information warfare doctrine? Third, at this time, how useful is Air Force information warfare doctrine for today's Air Force? To best answer these questions, this research paper examines the origin of Air Force information warfare doctrine in relation to information warfare theory and experience, the status of Air Force information warfare doctrine in comparison to sister service and joint information warfare doctrine, and the near-term usefulness of Air Force information warfare doctrine to Air Force members. The author concludes that the Air Force needs to publish its information warfare doctrine as soon as possible to help reduce the "fog" associated with this topic and to generate further discussion and development of the concepts and guidance in this critical area.

Chapter 1

Introduction

> *One of the four major trends seen by Air University in "Air Force 2025" is that "influence increasingly will be exerted by information more than by bombs." In "Joint Vision 2010," the Joint Chiefs of Staff specify the central operational concept of the future—the one from which the others will flow—to be information superiority*
>
> —John T. Correll
> "Warfare in the Information Age"
> *Air Force Magazine*

According to the *National Security Strategy*, the security of America's people, territory, and way of life, must be protected.[1] Consequently, the United States is to remain engaged in the world and to enlarge the community of secure, free market and democratic nations.[2] The strategy's three central goals are "to enhance our security with military forces that are ready to fight and with effective representation abroad, to bolster America's economic revitalization, and to promote democracy abroad."[3] The *National Security Strategy* further states:

> The emergence of the information and technology age presents new challenges to U.S. strategy even as it offers extraordinary opportunities to build a better future. This technology revolution brings our world closer together as information, money and ideas move around the globe at record speed; but it also makes possible for the violence of terrorism, organized crime and drug trafficking to challenge the security of our borders and that of our citizens in new ways.[4]

In order to achieve the national security strategy of engagement and enlargement, the *National Military Strategy* calls for flexible and selective engagement of US military power to assure the nation's security.[5] The three components of this strategy are "peacetime engagement, deterrence and conflict prevention, and fighting and winning our Nation's wars."[6] The strategy states that, in war, US military forces will follow several principles, one of which is "help dominate combat operations by winning the information war."[7] Why? Because modern reconnaissance, intelligence collection and analysis, and high speed data processing and transmission greatly enhance our ability to dominate warfare.[8] As the *National Military Strategy* states, "We must assure that this leverage works for us and against our adversaries."[9]

In *Joint Vision 2010, America's Military: Preparing For Tomorrow*, the Chairman of the Joint Chiefs of Staff detailed his vision for the future of US military forces. *Joint Vision 2010* is "the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."[10] The vision identifies four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics.[11] One vital aspect of the vision is the acknowledgment that:

> We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority will require both offensive and defensive information warfare.[12]

An illustration in *Joint Vision 2010* depicts the four operational concepts flowing from information superiority and resulting in massed effects.[13]

In addition to *Joint Vision 2010, C4I for the Warrior* continues as the enduring command, control, communications, computer, and intelligence (C4I) vision of the Joint Chiefs of Staff. Started in 1992, "C4I for the Warrior is a unifying concept that brings to the warrior an accurate and complete picture of the battle space, timely and detailed mission objectives, and the clearest view of the targets."[14] The 1995 progress report on this vision identified the growing importance of information warfare (IW), stating, "The use of advanced information systems and our increasing dependence on these systems leads to an increase in our vulnerability to adversary information warfare. IW is a warfare area defined by the target set of information, information based processes, and information systems. IW focuses on affecting an adversary's information environment while defending our own."[15]

Additionally, the October 1996 update to the *Air Force Executive Guidance* identified the core competencies of the USAF, one of which is information superiority. The document states that information superiority was the first core mission of the Air Force. This mission was initially accomplished as "early balloons and airplanes became spotters for Army commanders who were attempting to gain information to improve their decisions on the battlefield and gain advantage over an adversary."[16] The Secretary of the Air Force states, "Information is power. In today's turbulent international environment, knowledge of world events and secure information architectures are crucial if crises are to be averted or responded to quickly."[17] Emphasizing this position, the Chief of Staff of the Air Force stated, "Dominating the information spectrum is as critical now as occupying the land or controlling the air has been in the past."[18]

In November 1996, the Secretary of the Air Force and the Chief of Staff of the Air Force unveiled the new vision statement for the USAF, *Global Engagement: A Vision for the 21st Century Air Force.* "At the heart of Global Engagement is its commitment to fully integrate air and space into all Air Force operations and throughout its culture."[19] This vision is an outgrowth of the *National Security Strategy* and *Joint Vision 2010.* It places the Air Force in a position "to operate as a team within a joint team to meet the needs of the nation in the first quarter of the 21st century."[20] Once again, information superiority is listed as one of the core competencies of the Air Force. When referring to information superiority, *Global Engagement* states, "In no other area is the pace and extent of technological change as great as in the realm of information....Information Operations, and Information Warfare (IW) in particular, will grow in importance during the 21st century."[21]

Finally, in *C4I Horizon '95, A Vision for the Future*, the Air Force identifies its C4I vision as "Instant availability—to all military people and activities—of any information required for the execution of their mission."[22] *C4I Horizon '95* further states, "The war fighter in the 21st century must have unequivocal situational awareness. Such capability demands information dominance in the battle space and secure, reliable, and timely availability of all-source information for decision making. Exploitation and optimization of information technology are paramount to achieving this dominance and information operations will be the vehicle to achieve and sustain that purpose."[23]

This brief review clearly reveals how critical the military regards information dominance for future success in warfare. More specifically, information operations and information warfare play an ever-increasing role in the Air Force effectively participating

in military operations and, ultimately, in protecting the nation's security. But there are fundamental questions. First, what exactly is information warfare? Second, does the Air Force have or need information warfare doctrine, and, if so, why? Finally, what is the status of Air Force information warfare doctrine and how useful is the current Air Force information warfare doctrine? To best answer these questions, this research paper will examine the origin of Air Force information warfare doctrine in relation to information warfare theory and experience, the status of Air Force information warfare doctrine in comparison to sister service and joint information warfare doctrine, and the immediate usefulness of Air Force information warfare doctrine to Air Force members. Although not officially published, Air Force Doctrine Document (AFDD) 5, *Information Warfare*, October 1996, second draft, consolidates Air Force thinking about information warfare doctrine into a single document and is used for the assessment in this research paper.

Notes

[1] The White House, *A National Security Strategy of Enlargement and Engagement*, (Washington D.C.: U.S. Government Printing Office, February 1996), i.

[2] Ibid., ii.

[3] Ibid., i.

[4] Ibid., 1.

[5] Joint Chiefs of Staff, *National Military Strategy of the United States of America, A Strategy of Flexible and Selective Engagement*, (Washington D.C.: U.S. Government Printing Office, February 1995), 20.

[6] Ibid., i.

[7] Ibid., ii.

[8] Ibid., 15.

[9] Ibid.

[10] Joint Chiefs of Staff, *Joint Vision 2010, America's Military: Preparing For Tomorrow*, 1.

[11] Ibid.

[12] Ibid., 10.

[13] Ibid., 12.

[14] Joint Chiefs of Staff, *C4I for the Warrior, A 1995 Progress Report*, 1.

[15] Ibid., 21.

Notes

[16] Department of the Air Force, *Air Force Executive Guidance*, October 1996 Update, 20.

[17] Ibid.

[18] Ibid.

[19] Compiled from Air Force News Service and CSAF's Montgomery speech, "CSAF Unveils New Vision Statement at Strategic Force '96 Dinner," *Maxwell-Gunter Dispatch*, 22 November 1996.

[20] Ibid.

[21] Department of the Air Force, *Global Engagement: A Vision for the 21st Century Air Force*, 14.

[22] Department of the Air Force, *Horizon '95 C4I, A Vision for the Future*, 4.

[23] Ibid., 16.

Chapter 2

The Need for Air Force Information Warfare Doctrine

> *Those who are possessed of a definitive body of doctrine and deeply rooted convictions based upon it, will be in a much better position to deal with the shifts and surprises of daily affairs, than those who are merely taking short views, and indulging their natural impulses as they are evoked by what they read from day to day.*
>
> —Sir Winston Churchill

Before we assess Air Force information warfare doctrine, we need to answer some fundamental questions. First, what is information warfare and, second, what is doctrine and what are its basic uses?

What is Information Warfare?

As seen in the short review of the literature in the introduction, the term information warfare is widely used, but is it widely understood? The November 1995 USAF Fact Sheet, Information Warfare, correctly asserts, "There are many views on what constitutes information warfare."[1]

For example, in the 1995 *Cornerstones of Information Warfare*, the Air Force defined information warfare as:

> Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military functions."[2]

To better understand this definition, the document defined information as "data and instructions."[3] It then defined an information function as "any activity involving the acquisition, transmission, storage, or transformation of information."[4] Finally, it defined a military information function as "any information function supporting and enhancing the employment of military forces."[5] The document also defined information operations as "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces."[6]

A year later, in the October 1996 draft of AFDD 5, the Air Force defined information warfare as:

> Action taken within the information environment to deny, exploit, corrupt, destroy, or assure information viability.[7]

Shifting to another perspective, CJCS Instruction 3210.01, Joint Information Warfare Policy, 2 January 1996, defined information warfare as:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer based networks while defending one's own information, information-based processes, information systems and computer-based networks.[8]

From yet another perspective, the Army published Field Manual (FM) 100-6, *Information Operations*, in August 1996. In contrast with the Air Force and DOD, FM 100-6 states:

> The Army, recognizing that IW as currently defined by DOD is more narrowly focused on the impact of information during actual conflict, has chosen to take a somewhat broader approach to the impact of information on ground operations and adopted the term information operations. The Army adopted this broader approach to recognize that information issues permeate the full range of military operations (beyond just the traditional context of warfare) from peace through global war. IO implement the IW policy for the land component commander.[9]

In the 1996 study, *Strategic Information Warfare, A New Face of War*, RAND Corporation researchers concluded, "We recognize that for some time the term information warfare in common usage will have no more than a general meaning, and one that is recognized to be inescapably dynamic. Information warfare...is at a much too early stage of development or renewal to attempt to forge an agreed definition for the concept."[10]

In April 1996, the Joint Doctrine Working Party approved the project to produce Joint Pub 3-13, *Joint Doctrine for Information Warfare*.[11] The first draft of this joint publication was just released for coordination by the CINCs, Services, and Joint Staff. Interestingly, the title of the first draft was changed from *Joint Doctrine for Information Warfare* to *Joint Doctrine for Information Operations*. The publication proposes the following definitions:

> Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.
>
> Information Warfare: Information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[12]

The intent is to make a distinction between information operations and information warfare, with information warfare being a subset of information operations, conducted during times of crisis or conflict.

Obviously, the definition of information warfare has been in a state of flux. Joint Pub 3-13, when finally published, will go a long way toward establishing a firmer definition and clarifying the notions of information operations and information warfare. However, why has a definition of information warfare been so elusive? The answer to this question is

found in one's perspective and the implications and ramifications of any proposed definition. In 1995, General Fogleman astutely observed:

> Information warfare is not the exclusive domain of the Air Force, or any other service. I think information warfare has different meanings to a soldier, sailor, Marine or airman. For instance, the soldier's focus may be on what happens at the corps level and below. The sailor's and the Marine's focus is on the maritime and littoral regions. At the same time, an airman's focus is theater-wide, from the front lines to the adversary's capitol. You begin to see how IW covers the entire battlefield. But, because of these divergent views and unique needs, I think it's critical that all services come to grips with and develop capabilities for their respective mediums of operations—that is land, sea and air. Then, it falls to the joint force commander, or the regional commander-in-chief, to integrate these capabilities to accomplish the mission."[13]

Just as important as one's perspective are the implications and ramifications associated with the meaning of information warfare. As seen in the introduction to this paper, most would agree that information and information-based technology plays a critical and ever-increasing role in military operations. With the rapid advancements in information-based technology, the potential exists to dramatically improve military capabilities by exploiting the power of information in military operations. Some of the issues that quickly arise are what activities does information warfare include, who should be involved in information warfare, who has what responsibilities in information warfare, what limitations are there, if any, on information warfare, and a host of other issues. How these issues are handled obviously influences the definition of information warfare and the resulting doctrine.

Hoping to clarify these types of issues, the Joint Staff recently published the brochure, *Information Warfare, A Strategy for Peace...The Decisive Edge in War*, to "outline basic IW concepts and summarize ongoing initiatives implementing these concepts."[14] It

provides a concise synopsis of information warfare: "IW is an amalgam of warfighting capabilities integrated into a CINC's theater campaign strategy and applied across the range of military operations and all levels of war."[15] Further, the document states that "building information warfare means merging traditionally separate disciplines" such as intelligence, deception, computer security, counter intelligence, counter psychological operations (PSYOP), network management, electronic warfare, operations security, PSYOP, information attack, public affairs, counter deception, and physical deception.[16]

In a recent article in *Airpower Journal*, Major Richard C. Aldrich states, "Information warfare is believed by many to be the means by which the next 'big' war will be fought and, more importantly, the means by which future wars will be won. The term itself is enigmatic, embracing concepts as old as war itself and as new as the latest technology. The recent meteoric rise in prominence of the concept is inextricably linked to the dramatic advances in communications technology and information systems, specifically the computer."[17]

Despite all of the attention given to information warfare, there are critics who conclude that the rhetoric may be more hype than substance. One proponent of this viewpoint, Martin C Libicki, summarizes in his 1995 book, *What is Information Warfare?:*

> First, almost certainly there is less to information warfare than meets the eye. Although information systems are becoming more important, they are also becoming more dispersed and, if prepared, can easily become redundant....Second, information warfare has no business being considered as a single category of operations. Of the seven types of information warfare presented here, two—information blockade and cyberwarfare—are notional and the third—hacker warfare—although a real activity, is grossly exaggerated as an element of war viewed as policy by other means....Third, most of what U.S. forces can usefully do in information

> warfare will be defensive, rather than offensive. Much that is labeled information warfare is simply not doable—at least under rules of engagement the United States will likely observe for the foreseeable future.[18]

The intent here is to provide a general impression about some of the current thinking on the subject. Clearly, there is a flurry of activity occurring in this area. This is the direct result of the importance with which the military, including the Air Force, views information warfare. Since it is so significant, the Air Force needs to produce guidance on how to best go about conducting information warfare. This leads to the question, what is doctrine and what are its basic uses?

What is Doctrine?

Although countless books and articles have been written on the subject, perhaps the best starting point to answer this question is to examine current USAF doctrine, that is, AFM 1-1, dated March 1992. In the foreword to the manual, former Chief of Staff of the Air Force, General Merrill A. McPeak, states, "This manual is one of the most important documents ever published by the United States Air Force. Doctrine is important because it provides the framework for understanding how to apply military power. It is what history has taught us works in war, as well as what does not."[19] Further, the introduction to AFM 1-1 states:

> Aerospace doctrine is, simply defined, what we hold true about aerospace power and the best way to do the job in the Air Force. It is based on experience, our own and that of others. Doctrine is what we learned about aerospace power and its application since the dawn of powered flight....Thus, doctrine is a guide for the exercise of professional judgment rather than a set of rules to be followed blindly. It is the starting point for solving contemporary problems. Doctrine is also a standard against which to measure our efforts....Doctrine should be alive—growing, evolving, and

> maturing....If we allow our thinking about aerospace power to stagnate, our doctrine can become dogma.[20]

The glossary to AFM 1-1 states that basic doctrine "provides broad, enduring guidance which should be used when deciding how Air Force forces should be organized, trained, equipped, employed, and sustained"[21]

Additionally, General Fogleman expands on these basic thoughts in his recent article on doctrine in *Airpower Journal*. He asserts:

> Air Force doctrine should provide an integrating framework to tie together the various elements of the Air Force team, to show how these elements work together, and to provide the basis for integrating airpower with other forms of combat power in joint operations. While doctrine can be useful in intellectual debates and can provide a valid input for future programming, its primary purpose should be to guide war fighting and military operations other than war....The ultimate goal of our doctrine should be the development of an airman's perspective on joint warfare and national security issues—not just among generals, but among all airmen in all specialties.[22]

For purposes of this research paper on Air Force information warfare doctrine, what can we glean from these ideas about doctrine? Based on AFM 1-1 and General Fogleman's recent thoughts about doctrine, here are some basic characteristics of and uses for doctrine:

1. Provides the framework for understanding how to apply military power
2. Based on experience throughout history
3. Generally speaking, the best way to do the job
4. A guide rather than a strict set of rules
5. Starting point for solving present day problems and the standard for measuring efforts
6. Should be dynamic rather than static
7. The basis for organizing, training, equipping, employing, and sustaining forces
8. Defines relationships with other elements of the Air Force
9. Basis for integration with the "joint" team
10. Guides actions throughout the entire spectrum of military operations

These items can be grouped into three broad categories and applied to the issue of Air Force information warfare doctrine:

1. Fundamental concepts and ideas about information warfare
2. Relationships defined within the Air Force and for joint and multinational operations, providing the basis for organizing, training, equipping, employing, and sustaining forces
3. Guidelines, based on experience, since much of information warfare is not new, on how to conduct information warfare throughout the entire spectrum of military operations.

We should expect the official iteration of Air Force information warfare doctrine to contain these essential "ingredients."

To summarize, the question is why do we need Air Force information warfare doctrine? Despite the lack of a common definition for information warfare, it is clear that many concepts and disciplines that have existed for centuries are merging with the latest technological innovations to create a change in warfare. The best short answer to the question, why do we need Air Force information warfare doctrine, is found in the quote by Sir Winston Churchill at the beginning of this chapter. In essence, publishing Air Force information warfare doctrine forces the USAF to more fully address the subject of information warfare and to hopefully provide solid guidance to conduct information warfare in a methodical and controlled manner, rather than potentially in a haphazard and impulsive manner.

Notes

[1] USAF Fact Sheet 95-20, *Information Warfare*, November 1995.
[2] Department of the Air Force, *Cornerstones of Information Warfare*, 1995, 3.
[3] Ibid., 2.
[4] Ibid., 3.
[5] Ibid.
[6] Ibid., 11.

Notes

[7] Air Force Doctrine Document (AFDD) 5, *Information Warfare*, October 1996, Second Draft, 27.

[8] CJCSI 3201.01, *Joint Information Warfare Policy,* 2 January 1996.

[9] Field Manual (FM) 100-6, *Information Operations*, August 1996, 2-2.

[10] Richard C. Molander, Andrew S. Riddle, Peter A. Wilson, *Strategic Information Warfare, A New Face of War* (Santa Monica, CA: RAND, 1996), 1.

[11] "Joint Doctrine Working Party," *Joint Force Quarterly*, Spring 96, 128.

[12] Joint Pub 3-13, *Joint Doctrine for Information Operations*, 21 January 1997, First Draft, GL-11.

[13] General Ronald R. Fogleman, "Fundamentals of Information Warfare - An Airman's View," address presented to the National Security Industry Association-National Defense University Foundation Conference on the Global Information Explosion, Washington, D.C., May 16, 1995.

[14] Joint Chiefs of Staff, *Information Warfare, A Strategy for Peace....The Decisive Edge in War*, front cover.

[15] Ibid., 2.

[16] Ibid., 17.

[17] Major Richard W. Aldrich, "The International Legal Implications of Information Warfare," *Airpower Journal*, Fall 1996, 99.

[18] Martin C. Libicki, *What Is Information Warfare?*, (National Defense University, August 1995), 96, 97.

[19] Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992, v.

[20] Ibid., vii.

[21] Ibid., vol. 2, March 1992, 274.

[22] General Ronald R. Fogleman, "Aerospace Doctrine—More Than Just a Theory," *Airpower Journal*, Summer 1996, 41, 46.

Chapter 3

The Fundamentals

> *When Basic Aerospace Doctrine of the United States Air Force was last published, in March 1992, it did not even include 'information warfare' in the forty-page glossary. The closest it came to recognizing information warfare was to list surveillance, reconnaissance, and electronic combat as 'force enhancement' missions. Since then, the conceptual universe has shifted.*
>
> —John T. Correll,
> "Warfare in the Information Age"
> *Air Force Magazine*

As stated in the introduction to this paper, the second draft of AFDD 5 provides the basis for examining the usefulness of Air Force information warfare doctrine in the next three chapters. The first area to examine is the fundamental concepts and ideas about information warfare.

The foreword to the draft AFDD 5 sets the stage for this discussion:

> Information has long been an integral component of warfare. Human competition necessitates knowing one's adversary, affecting opponents' perceptions, and safe-guarding sensitive information. History is replete with examples of how important information has been in political and military struggles—from the earliest battles described in the Epic of Gilgamesh to current operations in Bosnia. Information warfare (IW)—the exploitation of an information advantage over an adversary—has raised the importance of information in successful military operations to a crucial level.
>
> IW is not platform dependent. It is not an operation or a mission. Nor is it confined to a particular degree of hostilities on the spectrum of military operations. The fundamentals of IW—attacking an opponent's information

> while achieving friendly information assurance—have not changed through time. What has changed is the means of affecting the adversary's perception and will. Additionally, today's information environment presents inherent capabilities and liabilities to friendly forces heretofore unknown.[1]

In particular, Chapter 2 of the draft AFDD 5 defines basic terminology and lays the conceptual foundation for the remainder of the doctrine document. Of particular interest in that chapter is a diagram illustrating the prominent information warfare activities. The diagram shows the overarching concept of information warfare and breaks it down into its components.[2]

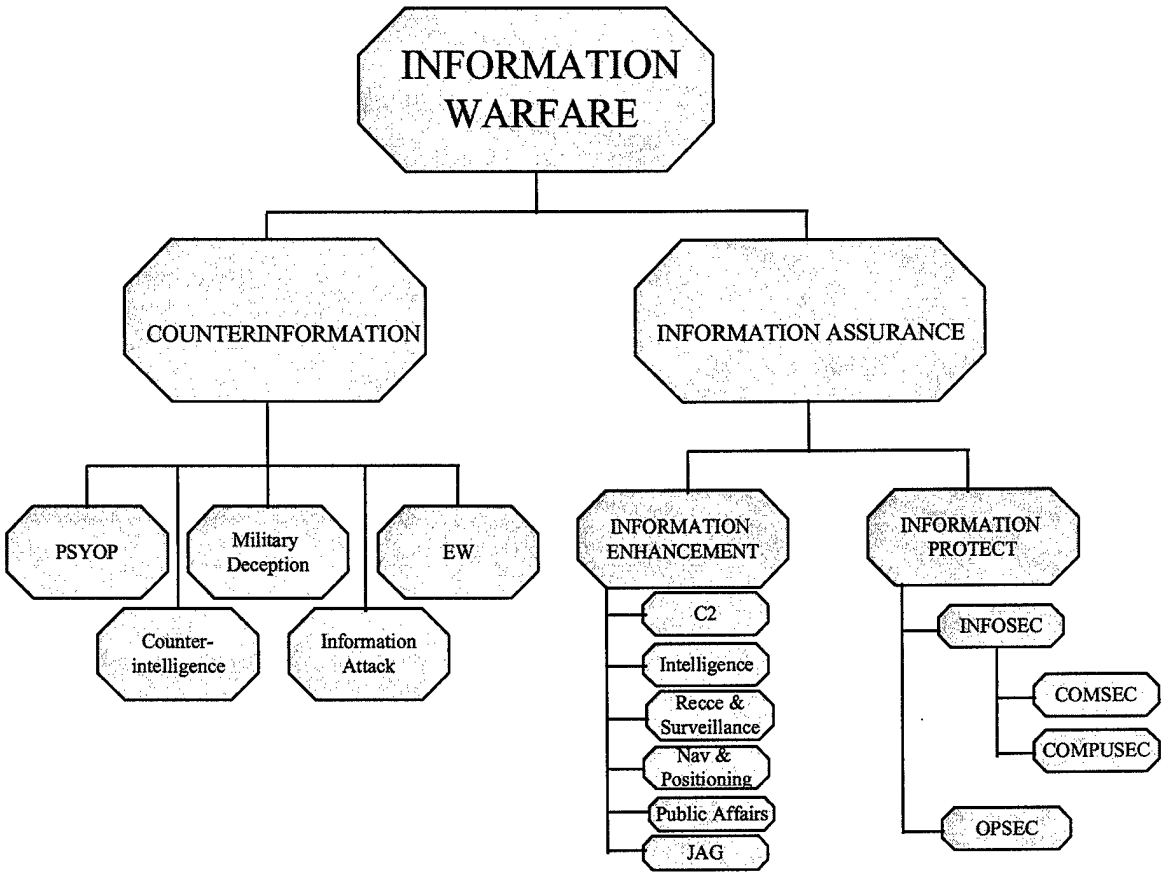

Figure 1. Prominent Information Warfare Activities

The two major areas under information warfare are counterinformation and information assurance. Counterinformation corresponds to the familiar Air Force doctrinal concepts of counterair and counterspace. In the same way, counterinformation seeks to "create an environment where friendly forces can conduct operations with some degree of freedom of action, while simultaneously denying the adversary the ability to conduct those operations against friendly forces."[3]

There are several areas of Air Force operations that seek to deny, exploit, corrupt, or destroy an adversary's information and its functions: psychological operations (PSYOP), military deception, electronic warfare (EW), information attack, and counterintelligence. Some of these areas are not new and have been performed by the Air Force since its inception. However, the conceptual shift here is that these areas will be fused into the overarching "umbrella" of information warfare. By using the various components in concert with each other, military information operations can produce synergistic effects beyond their individual capabilities.

One area in particular, information attack, indicates the need for a way to exploit the vulnerability of modern day information systems. According to the AFDD, "information attack encompasses activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides."[4] For example, such operations would manipulate data bases which can lead to the use of incorrect information by enemy decision makers. This could result in a loss of confidence in their information systems or, more significantly, in detrimental consequences on the battlefield. Obviously, legal considerations must be kept in mind when conducting information attack.

The other major area under information warfare is information assurance, consisting of "measures to enhance and protect friendly information and functions."[5] This area is broken down into information enhancement and information protection. "Information enhancement, the organized network of information functions that enhance force employment, is critical to today's global engagement requirements. Information protection, designed to safeguard equipment and information, can prohibit unintentional and unwanted release of information."[6] It's interesting to note that information enhancement includes command and control, intelligence, reconnaissance and surveillance operations, precision navigation and positioning, public affairs, and legal considerations. Information protection includes information security, communications security, computer security, and operations security. "Information protect activities occur within the context of four interrelated processes: information environment security, attack detection, attack response, and capability restoration."[7] Again, most of these areas are not new areas of operations. However, by merging these efforts under information warfare, information can be used to increase military capabilities and gain an advantage over an adversary.

Although AFDD 5 does provide an overarching conceptual framework for Air Force information warfare operations, it is lacking in some areas. First, the draft Air Force doctrine document needs to clarify the distinction developing in joint doctrine between information operations and information warfare. Currently, the draft document does not define information operations. In the case of the Air Force, the term information warfare connotes that although we, as a nation, may be in a state of peace, any activity conducted in the information dimension is included under the broad heading of information warfare. This presents a potential problem when conducting military operations in an environment

other than war. By using the term information warfare exclusively and not providing for a less provocative term, when not at war, allies, coalition partners, government agencies, non-governmental organizations, and others can interpret activities termed as information warfare as having some type of hostile intent. Obviously, in this type of environment, this could very easily result in counterproductive attitudes and, consequently, counterproductive actions. For example, when working with non-governmental organizations and private voluntary organizations during joint operations, joint doctrine warns against conveying the impression to these organizations that they are just another source of intelligence. Rather, they should be treated as partners who choose to share information to help achieve mutually agreed upon goals.[8] In similar fashion, the Air Force needs to develop terminology to make critical distinctions in their information activities so as not to produce unintended effects. One simple solution is to make the distinction that draft Joint Pub 3-13 and FM 100-6 are making about information operations and information warfare.

Second, the document could be improved by expanding on the information environment present in the world today. For example, draft Joint Pub 3-13 discusses the various information infrastructures that are inseparably linked together. It states, "Open and interconnected systems are coalescing into a rapidly expanding global information infrastructure (GII) that enfolds the US National Information Infrastructure (NII) and the DOD Defense Information Infrastructure (DII)."[9] This is a significant point for military activities in that the DII is deeply embedded in the NII. For instance, the DII relies heavily on national telecommunications networks, a variety of information databases, and satellite communications networks. This reliance has dramatic implications for the military.

Military operations are vulnerable to disruptions in the NII, creating the need to work with government agencies and industry to protect against attacks on these systems. To highlight this point, a 1996 Air Command and Staff College research paper identified the following statistics: "The Defense Information Systems Agency reported that in 1994 there were 238 reported break-ins to DOD systems resulting in data and software destruction/modification. Testing over 8900 computer hosts showed 88% of unclassified DOD computers were penetrated with 96% of the penetrations undetected by the host. Of those detected, 95% were unreported. Widely accepted estimates indicate over 90% of DOD information transits commercial information paths; combine this with increased availability of computer 'weaponry' to the masses, and the need for appropriate defensive measures is obvious."[10] Air Force members need to understand these interrelationships and the vulnerabilities inherent in the integration of these infrastructures.

Third, the Air Force doctrine document also needs to include a discussion about information warfare objectives at the strategic, operational, and tactical levels. For instance, draft Joint Pub 3-13 states, "The human and associated decision-making processes are the ultimate target for offensive IO. Offensive IO are employed as an integrating strategy that orchestrates varied disciplines and capabilities into a coherent, seamless plan to achieve specific objectives."[11] This should include such objectives as deter war, affect infrastructure, disrupt WMD program, support peace operations, expose enemy deception, decapitate enemy NCA and military commanders from forces, disintegrate integrated air defense system, and destroy or degrade tactical command and control.[12]

Fourth, Air Force information warfare doctrine should also include such areas as physical security and network management, including their respective definitions and descriptions of their areas of operations. For example, the Base Network Control Center concept is taking on increased significance in the Air Force. This not only allows Air Force bases to improve their ability to detect information attacks being conducted against Air Force information assets, but also to develop better measures for defending against such attacks.

Overall, though the draft Air Force information warfare doctrine document identifies and explains fundamental concepts and ideas about information warfare, there are areas for improvement. Air Force information warfare doctrine needs to provide a more complete picture of the information environment and make vital distinctions concerning the terminology used to describe information activities throughout the entire spectrum of military operations.

Notes

[1] Air Force Doctrine Document (AFDD) 5, *Information Warfare*, October 1996, Second Draft, I.

[2] Ibid., 3.

[3] Ibid., 4.

[4] Ibid., 5.

[5] Ibid., 6.

[6] Ibid.

[7] Ibid., 10-11.

[8] Joint Pub 3-08, *Interagency Coordination During Joint Operations*, Vol. 1, 9 October 1996, III-13.

[9] Joint Pub 3-13, *Joint Doctrine for Information Operations*, 21 January 1997, First Draft, I-23.

[10] Lt Col Sweed Faisal Al-Ajmi et al., "Does the Air Force Need Information Warfare Units?," Research Paper no. 96-126 (Maxwell AFB, Ala.: Air Command and Staff College, 1996), 2.

[11] Joint Pub 3-13, II-1.

[12] Ibid., II-3.

Chapter 4

The Relationships

IW is a reality today and in the future; it impacts societies, governments, and the range of military operations, and all levels of war.

—The Joint Staff
Information Warfare, A Strategy for Peace....The Decisive Edge in War

Chapters 3 through 6 of the second draft of AFDD 5 identify relationships within the Air Force and also for joint or multinational operations. In particular, the primary entities mentioned in the document are the Air Force Information Warfare Center (AFIWC), the Information Warfare Squadron (IWS), the Air Force Computer Emergency Response Team (AFCERT), and the information warfare coordination cells.

"The AFCERT was established as the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities. The AFCERT, consisting of Air Force Information Warfare Center (AFIWC) personnel, will coordinate the technical resources of AFIWC to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities reported by Air Force computer users, security managers, and system managers."[1] As part of the information protect aspect of information warfare, the draft document describes a process for base Computer Security Officers to report Air Force computer security incidents through the Major Command (MAJCOM) Computer System Security Manager (MCCSSMM) to the AFCERT. The

purpose of this process is to "ensure MAJCOM operational and support systems are fully capable of meeting the objectives set forth in applicable mission statements, operation plans, and other pertinent requirements documents."[2] The Information Warfare Squadron, established in 1995, "provides similar support and services to in-theater forces as the AFCERT does in the continental US....The IWS deploys augmentation forces to the theater to support IP operations."[3]

Additionally, information warfare relationships are necessary for joint and multinational operations. "The key to successful information warfare is its integration throughout the planning, executing, and terminating phases of all joint and multinational operations. This requires coordination between all in-theater operations....The JFACC maintains awareness of an adversary's information infrastructure, capabilities, and operations through an IW cell within the air operations center (AOC) composed of IW planners and liaison personnel. A notional IW cell may include military deception, PSYOP, information protect, intelligence, information attack experts, counterintelligence, EW, air operations, and other expertise deemed necessary."[4] The information warfare cell develops information warfare strategies and makes target recommendations as necessary for strategic attack and interdiction. For strategic attack, this may include Voice of America television broadcasts to influence public support for a leader and weaken the national will to engage in conflict. For interdiction, this may include information attack to "manipulate enemy information directing follow on troops into a theater of operations and send troops to another location. Databases could also be corrupted, resulting in misallocation of supplies and material."[5]

On a broader national level, Air Force information warfare assistance may be provided to law enforcement agencies (LEAs). "In the case of attacks against military and civilian information systems through the INTERNET, the military may provide assistance to LEAs under certain conditions. Detection of information system intrusions may occur as collateral information obtained by the military in conjunction with information protection programs. This information may be shared with LEAs when necessary to protect critical civilian property and functions. In the event of a civil disaster that may endanger normal governmental functions, the federal government, applying emergency authority, may use military capabilities to determine perpetrators' motives and means of system intrusion."[6]

The draft doctrine document, however, has some glaring omissions. First, and most importantly, the document does not have an organizational chart to identify key Air Force information warfare organizations, entities, and units, and their respective responsibilities. The doctrine would be much clearer if it included this information. For example, the 1996 Air Command and Staff College research paper, *Does the Air Force Need Information Warfare Units?*, provides an excellent summary of the various Air Force organizations specifically involved in information warfare activities. This includes Headquarters Air Force Plans and Operations (XO) directorate (the designated lead agent for information warfare within the Air Force), certain offices within the Intelligence, Communications, and Acquisition directorates, Air Intelligence Agency (with the mission to provide multi-source intelligence products, applications, services, and resources in the area of information warfare/command and control warfare (IW/C2W), security, acquisition, foreign weapons systems and technology, and treaty monitoring), the National Air

Intelligence Center (NAIC) under AIA (can provide the war fighter a concise information package tailored to meet a threat), 67th Intelligence Wing (managing the Air Force's planning of all-source intelligence, information warfare, and security support), and more.[7] Obviously, the recent reorganization of the Air Staff has changed some of the specific offices. However, the point here is that an organizational chart, including a brief explanation of the organization's role and the support that can be provided to other Air Force units would add immeasurably to the final doctrine document.

Also, the draft document fails to identify some key organizations that the Air Force must work with to conduct information warfare. First, the Defense Information Systems Agency (DISA) ensures measures are taken to protect the Defense Information Infrastructure. DISA is also responsible for minimizing duplication of effort in this area thought the DOD. Therefore, Air Force members can interface with DISA on information protection issues. Second, the National Security Agency provides information systems security technology, products, and services to help protect against hostile information warfare. Third, the relationship between Air Force MAJCOMs is limited almost exclusively to computer security. Again, information warfare encompasses much more than this one element and the relationships in the numerous other operational areas should be identified and described.

Overall, the draft Air Force information warfare doctrine document identifies several key relationships for information warfare activities, within the Air Force and for joint and multinational operations, and briefly describes the organizational structure required to conduct information warfare. The document needs to add an organizational chart and to include some key national-level organizations that Air Force members can expect to work

with during their daily information warfare operations. Finally, the published doctrine needs to further describe the relationships within and between MAJCOMs, beyond just the computer security arena currently mentioned.

Notes

[1] Air Force Doctrine Document (AFDD) 5, *Information Warfare*, October 1996, Second Draft, 13.

[2] Ibid., 14.

[3] Ibid., 15.

[4] Ibid., 16.

[5] Ibid., 17, 18.

[6] Ibid., 21.

[7] Lt Col Sweed Faisal Al-Ajmi et al., "Does the Air Force Need Information Warfare Units?," Research Paper no. 96-126 (Maxwell AFB, Ala.: Air Command and Staff College, 1996), 24-27.

Chapter 5

The Guidelines

> *What is doctrine? Simply this: doctrine is officially approved prescriptions of the best way to do a job. Doctrine is, or should be, the product of experience. Doctrine is what experience has shown usually works best*
>
> —Maj Gen I.B. Holley
> *Of Saber Charges, Escort Fighters, and Spacecraft, The Search for Doctrine*

The second draft of AFDD 5 addresses the fundamentals and relationships necessary to conduct information warfare. With the suggested improvements, the document can be even clearer and more comprehensive. However, the document provides virtually no guidance on how to conduct information warfare. As previously stated, information warfare incorporates many activities that are not new to military operations, including such areas as psychological operations, military deception, electronic warfare, counterintelligence, command and control, intelligence, reconnaissance and surveillance, information security, communications security, computer security, operations security, public affairs, and legal considerations. The doctrine document defines and describes these areas but gives few guidelines and examples on how to actually conduct operations in these areas. Additionally, the document describes the information warfare coordination cell and its roles in Air Force, joint, and multinational operations. However, it must include guidance on how to use information warfare throughout the entire spectrum of

military operations, from peace to general war, how to actually conduct an information warfare campaign, and how the activities relate to the overall effort of the supported commander-in-chief.

Information Warfare Campaign Planning

Draft AFDD 5 states, "The JFACC maintains awareness of an adversary's information infrastructure, capabilities, and operations through an IW cell within the air operations center (AOC) composed of IW planners and liaison personnel. A notional IW cell may include military deception, PSYOP, information protect, intelligence, information attack experts, counterintelligence, EW, air operations, and other expertise deemed necessary. The IW cell develops IW strategies and makes target recommendations as necessary."[1] The document does not provide any substantive guidance on how this should be accomplished.

Interestingly, the draft Joint Pub 3-13 includes a chapter titled Information Operations Organization. The critical information operations (IO) organization is the IO cell. The draft doctrine states, "A fully functional IO cell is paramount to successful IO. The IO cell integrates the broad range of potential IO actions and activities that help contribute to the commander's desired end state in an AOR or JOA. The organizational structure to plan and coordinate IO should be sufficiently flexible to accommodate a variety of planning and operational circumstances. This chapter focuses on how to organize to plan to execute IO."[2] Obviously, the Air Force may have considerable representation in the cell. The publication includes a diagram to identify resident and nonresident members of a typical joint IO cell. The diagram includes the IO officer (J3), and representatives from J2, J5, J6,

J7, Public Affairs, Staff Judge Advocate, counterintelligence, civil affairs, service components, targeting, special operations, information attack, special technical operations, electronic warfare, psychological operations, military deception, operations security, and others such as US Space Command and Defense Information Systems Agency.[3] This is mentioned here to show the potential robustness of conducting offensive and defensive information warfare in a joint and multinational environment. Air Force representation will not be limited to an AOC under the JFACC, as mentioned in the draft Air Force doctrine.

The key point here is that information activities are not limited to the air and space medium. Does the Air Force limit its participation solely to this medium or ultimate effects in this medium? For example, suppose the information warfare cell in the air operations center is developing its target list. Based on the stated objectives and strategies developed for an operation, a target may be to disrupt the activities of an enemy communications center. This could be accomplished by either an air strike or an information attack to ruin its software or sever its communications connectivity. In this case, an aircraft sortie may not be required and the means for conducting the information attack is an Air Force special operations team. Therefore, to conduct this form of warfare, there is virtually no interaction required with the air tasking order planning. The conclusion here is that information warfare is altering the traditional lines of responsibility for campaign planning and new structures and relationships must be developed. The information warfare cell under the Joint Force Air Component Commander and the information operations cell under the Joint Force Commander are attempts to

accommodate the changes being brought about as a result of information warfare considerations.

One way to address the issue of information warfare campaign planning is to determine the essential elements of campaign planning and use them in whatever organizational structure is established to conduct actual information warfare operations. In the 1996 Air Command and Staff College research paper, *Information Warfare: Planning the Campaign*, the researchers concluded there are five essential functions required to conduct an information warfare campaign: survey, assess, command, control, and execute.[4] Survey is the function to accumulate data about the opponent's information system.[5] Assess is the function to process and analyze the data accumulated in the survey step.[6] Command is the function to conduct planning and determine courses of action. This includes matching specific information warfare tools to centers of gravity identified in the assess step.[7] Control is the function that "analyzes received tasking orders, readies assets, responds to the threat and situational changes, and reports the results back through the chain of command."[8] Execute is the function that includes both facets of information warfare, that is, information attack and information protect. The research paper identifies six categories of operations that can be employed to attack or defend information (again, many of these operational forms are not new in the military)[9]:

1. Psychological operations: Use of information to affect the enemy's reasoning
2. Electronic warfare: Denies the enemy accurate information
3. Military deception: misleads the enemy about one's capabilities or intentions
4. Physical destruction: converts stored energy to destructive power
5. Security measures: denies information on military capabilities and intentions
6. Information attack: directly corrupts information without visibly changing the physical entity within which it resides.

Obviously, at the present time, the assets of the air, land, and sea components will be employed to execute the desired missions, but the centralized planning of the information warfare cell distributes the target information to the respective components for decentralized execution.

Another model for developing an information warfare campaign is the joint air operation planning process found in Joint Pub 3-56.1, *Command and Control for Joint Air Operations*. The pub describes a 5-phase planning process (operational environment research, objective determination, strategy identification, center(s) of gravity (COG) identification, joint air operations plan development) that culminates in a detailed air operations plan.[10] In similar fashion, a joint information warfare operation plan could be developed and then execution would be conducted by the respective war fighters from the various components.

Finally, there needs to be a link between Air Force information warfare planning and deliberate and crisis action planning. Sample annexes and applicable appendices should be developed to aid planners in developing the information warfare campaign and incorporated into Joint Operation Planning and Execution System (JOPES).

Overall, the draft Air Force information warfare doctrine document provides very little guidance on how to conduct information warfare operations within the Air Force and for joint and multinational operations. This significant shortcoming can be dramatically improved by incorporating the essentials for successful information warfare campaign planning, from critical functions that apply to every information warfare campaign to a detailed campaign plan with the associated target list for execution. Additionally, this

planning must be integrated into the existing deliberate and crisis action planning processes and the Joint Operations Planning and Execution System (JOPES).

Notes

[1] Air Force Doctrine Document (AFDD) 5, *Information Warfare*, October 1996, Second Draft, 16.

[2] Joint Pub 3-13, *Joint Doctrine for Information Operations*, 21 January 1997, First Draft, IV-1.

[3] Ibid., IV-4.

[4] Lt Col Frederick Okello et al., "Information Warfare: Planning the Campaign," Research Paper no. 96-124 (Maxwell AFB, Ala.: Air Command and Staff College, 1996), 48.

[5] Ibid., 49.

[6] Ibid., 52.

[7] Ibid., 53.

[8] Ibid., 54.

[9] Ibid., 55.

[10] Joint Pub 3-56.1, *Command and Control for Joint Air Operations*, 14 November 1994, Chapter 3 and Appendix A.

Chapter 6

Conclusion

> *Warfare in the information age carries us into uncharted territory. We will find new opportunities there, as well as dangers that we will not expect or fully understand. The objectives are not yet clear, and the problems we do see will almost certainly change before we can resolve them. The best we can do is to stay alert and flexible, equip ourselves with the best technology we can muster, and go forward with all the capabilities and options that we can muster.*
>
> —John T. Correll,
> Warfare in the Information Age
> *Air Force Magazine*

Information warfare is rapidly mounting in significance, both in the military, as a whole, and the Air Force, in particular. General Shalikashvili recently concluded, "Information Warfare (IW) has emerged as a key joint warfighting mission area. The explosive proliferation of information-based technology significantly impacts warfighting across all phases, the range of military operations, and all levels of war....When fully developed and integrated, IW offers enormous potential to support our warfighters."[1] In order to fully exploit the potential of information warfare, the Air Force must publish information warfare doctrine as soon as possible. This doctrine, at a minimum, must be comprehensive enough to explain fundamental concepts and ideas about information warfare, define basic relationships within the Air Force and for joint and multinational operations, and clearly express guidelines, based on experience, on how to conduct

information warfare throughout the entire spectrum of military operations. As additional experience is gained in this area, the doctrine can be updated to incorporate valuable lessons learned and, therefore, keep pace with the technological and strategic changes continuously emerging in the world.

By publishing Air Force information warfare doctrine, a benchmark can be established to educate Air Force members about the role of and means for conducting information warfare and also to encourage discussion for generating useful ideas and concepts on how to better conduct information warfare throughout the entire spectrum of military operations. In so doing, the Air Force can do its part to help reduce the "fog" associated with this subject. By incorporating the suggested recommendations of this research into the officially published doctrine document, then Air Force information warfare doctrine can and will be valuable to Air Force members in and for the near-term future.

In conclusion, this research paper makes the following recommendations to improve the draft Air Force information warfare document.

Fundamental concepts and ideas about information warfare:

1. Distinguish between information operations and information warfare, since the Air Force will participate in military operations other than war
2. Expand the description of the information environment that the Air Force participates in, since it is extremely reliant on the global information infrastructure and the national information infrastructure
3. Describe typical information warfare objectives at the strategic, operational, and tactical levels, since objectives drive strategies and, ultimately, execution
4. Incorporate such areas as physical security and network management, including their respective definitions and descriptions of their areas of operations, since these areas are already intertwined with other information warfare considerations

Relationships defined within the Air Force and for joint and multinational operations, providing the basis for organizing, training, equipping, employing, and sustaining forces:

1. Include a diagram to identify key Air Force information warfare organizations and their respective responsibilities (including such organizations as Air Staff, information warfare centers, information warfare squadrons, information warfare cells under the joint force commander and joint force air force component commander, and base network control centers), since Air Force members need to understand the organizational structure the Air Force uses to conduct information warfare and where they can get support, if required
2. Include some additional key organizations that the Air Force must work with to conduct information warfare, since Air Force members can expect to interact with them at various times
3. Describe the relationships within and between MAJCOMs in all areas of information warfare, since there is more to information warfare than just the computer security arena currently emphasized

Guidelines, based on experience, since much of information warfare is not new, on how to conduct information warfare throughout the entire spectrum of military operations:

1. Define the essential functions required to conduct a successful information warfare campaign, regardless of the organizational structure, since Air Force members will be expected to operate in a variety of information warfare environments
2. Devise a process to develop a detailed information warfare campaign plan with the associated target list for execution, since this is the means for executing the objectives and strategies identified for any military operation
3. Integrate information warfare campaign planning into the existing deliberate and crisis action planning processes and incorporate it in the Joint Operations Planning and Execution System (JOPES), since these are the processes Air Force members use to plan for military operations.

Notes

[1] Joint Chiefs of Staff, *Information Warfare, A Strategy for Peace....The Decisive Edge in War*, Preface.

Bibliography

Air Force Doctrine Document (AFDD) 5. *Information Warfare*, October 1996, Second Draft.

Air Force Manual (AFM) 1-1. *Basic Aerospace Doctrine of the United States Air Force.* 2 vols., March 1992.

Al-Ajmi, Lt Col Sweed Faisal, et al. "Does the Air Force Need Information Warfare Units?" Research Paper no. 96-126. Maxwell AFB, Ala.: Air Command and Staff College, 1996.

Aldrich, Major Richard W., "The International Legal Implications of Information Warfare," *Airpower Journal*, Fall 1996.

CJCS Instruction 3201.01, *Joint Information Warfare Policy*, 2 January 1996.

Correll, John T., "Warfare in the Information Age," *Air Force Magazine*, December 1996, 3.

Department of the Air Force, *Air Force Executive Guidance*, October 1996 Update.

Department of the Air Force, *Cornerstones of Information Warfare*, 1995.

Department of the Air Force, *Global Engagement: A Vision for the 21st Century Air Force.*

Department of the Air Force, *Horizon '95 C4I, A Vision for the Future*, 1995.

Field Manual (FM) 100-6. *Information Operations*, August 1996.

Fogleman, General Ronald R., "Aerospace Doctrine—More Than Just a Theory," *Airpower Journal*, Summer 1996, 40-47.

Fogleman, General Ronald R., "Fundamentals of Information Warfare—An Airman's View," address presented to the National Security Industry Association-National Defense University Foundation Conference on the Global Information Explosion, Washington, D.C., May 16, 1995.

Holley, Major General I.B., Jr., "Of Saber Charges, Escort Fighters, and Spacecraft, The Search for Doctrine," *Air University Review*, October 1983, 2-11.

Joint Chiefs of Staff, *C4I for the Warrior—A 1995 Progress Report.*

Joint Chiefs of Staff, *Information Warfare, A Strategy for Peace....The Decisive Edge in War.*

Joint Chiefs of Staff, *Joint Vision 2010, America's Military: Preparing For Tomorrow.*

Joint Chiefs of Staff, *National Military Strategy of the United States of America, A Strategy of Flexible and Selective Engagement*, Washington D.C.: U.S. Government Printing Office, February 1995.

"Joint Doctrine Working Party." *Joint Force Quarterly*, Spring 96.

Joint Pub 3-08. *Interagency Coordination During Joint Operations.* 2 vols., 9 October 1996.

Joint Pub 3-13. *Joint Doctrine for Information Operations*, 21 January 1997, First Draft.

Joint Pub 3-56.1. *Command and Control for Joint Air Operations*, 14 November 1994.
Libicki, Martin C., *What Is Information Warfare?* National Defense University, August 1995.
Maxwell-Gunter Dispatch, 22 November 1996.
Molander, Richard C., Andrew S. Riddle, Peter A. Wilson. *Strategic Information Warfare, A New Face of War*. Santa Monica, CA: RAND, 1996.
Okello, Lt Col Frederick, et al. "Information Warfare: Planning the Campaign." Research Paper no. 96-124. Maxwell AFB, Ala.: Air Command and Staff College, 1996.
USAF Fact Sheet 95-20, *Information Warfare*, November 1995.
The White House, *A National Security Strategy of Enlargement and Engagement*, Washington D.C.: U.S. Government Printing Office, February 1996.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112